

We Claim:

1. A firewall for Internet protocol packets carrying data for a real-time Internet application, each of said 5 Internet protocol packets being associated with any one of a signaling channel, a control channel, or a bearer channel of said real-time Internet application, the firewall comprising:

an application proxy and a packet filter,

10

the firewall applying the Internet protocol packets associated with the signaling channel and the control channel to the application proxy, and the firewall applying the Internet protocol packets associated with the bearer channel to the 15 packet filter.

2. The firewall of claim 1 wherein said real-time Internet application is Voice over Internet Protocol (VoIP).

20 3. The firewall of claim 1 wherein said real-time Internet application is fax over Internet.

4. The firewall of claim 1 wherein said real-time Internet application is video over Internet.

25

5. The firewall of claim 1 wherein said real-time Internet application is voice messaging over Internet.

6. The firewall of claim 1 wherein the application proxy 30 instructs the packet filter as to which Internet protocol packets associated with a particular bearer channel to enable and disable for the duration of a session of said real-time Internet application.

7. The firewall of claim 1 further including a Network Address Translation (NAT) process to translate any Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) port numbers or User Datagram Protocol (UDP) port numbers contained at layer 3 and layer 4 of the Internet protocol packets associated with the signaling channel, the control channel and the bearer channel.

8. The firewall of claim 1 further including a Network Address Translation (NAT) process to translate any Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) port numbers or User Datagram Protocol (UDP) port numbers contained at layer 7 of the Internet protocol packets associated with the signaling channel and the control channel.

15 9. The firewall of claim 8 wherein said application proxy instructs said NAT process to operate for the duration of a session of said real-time Internet application independent of data traffic flow.

20 10. The firewall of claim 1 further including a control logic process for specifying the operating parameters of the firewall.

25 11. The firewall of claim 1 wherein said application proxy and said packet filter are housed in any one of a dual homed commercial workstation, a general purpose workstation, a dedicated hardware firewall appliance, or an application specific integrated circuit.

30 12. A method of protecting a computer network transmitting and receiving Internet protocol packets formatted in accordance with a real-time Internet protocol, each of said Internet protocol packets being associated with any one of a

09621260 - 092800

signaling channel, a control channel, or a bearer channel, the method comprising the steps of:

i. receiving a stream of Internet protocol packets,

5 ii. applying the Internet protocol packets associated with the signaling channel and the control channel to the application proxy, and

iii. applying the Internet protocol packets associated with the bearer channel to the packet filter.

10

13. The method of claim 12 further comprising the step of the application proxy instructing the packet filter as to which bearer channels to enable and disable for the duration of an Internet application session utilizing said real-time Internet protocol.

15

14. The method of claim 12 further comprising the step of applying a NAT process to translate any Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) port numbers or 20 User Datagram Protocol (UDP) port numbers contained at layer 3 and layer 4 of the Internet protocol packets associated with the signaling channel, the control channel and the bearer channel.

25

15. The method of claim 12 further comprising the step of applying a NAT process to translate any Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) port numbers or User Datagram Protocol (UDP) port numbers contained at layer 7 30 of the Internet protocol packets associated with the signaling channel and the control channel.

16. The method of claim 14 further comprising the step of the application proxy instructing the NAT process to operate for the duration of an Internet application session utilizing

00000000000000000000000000000000

said real-time Internet protocol independent of data traffic flow.

17. A computer readable medium containing computer
5 instructions for protecting an Internet Protocol network
transmitting and receiving Internet protocol packets formatted
in accordance with a real-time Internet protocol, each of said
Internet protocol packets being associated with any one of a
signaling channel, a control channel, or a bearer channel, said
10 computer readable medium comprising computer program code,
executable by a computer, for:

i. receiving a stream of Internet protocol
packets,

ii. applying the Internet protocol packets
15 associated with the signaling channel and the control channel
to the application proxy, and

iii. applying the Internet protocol packets
associated with the bearer channel to the packet filter.

18. The computer readable medium of claim 17 further
comprising computer program code, executable on a computer, for
the application proxy to instruct the packet filter as to which
bearer channels to enable and disable for the duration of an
Internet application session utilizing said real-time Internet
25 protocol.

19. The computer readable medium of claim 17 further
comprising computer program code, executable on a computer, for
a NAT process, and for applying the NAT process to translate
30 any Internet Protocol (IP) addresses, Transmission Control
Protocol (TCP) port numbers or User Datagram Protocol (UDP)
port numbers contained at layer 3 and layer 4 of the Internet
protocol packets associated with the signaling channel, the
control channel and the bearer channel.

20. The computer readable medium of claim 17 further comprising computer program code, executable on a computer, for a NAT process, and for applying the NAT process to translate
5 any Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) port numbers or User Datagram Protocol (UDP) port numbers contained at layer 7 of the Internet protocol packets associated with the signaling channel and the control channel.

10

21. The computer readable medium of claim 21 further comprising computer program code, executable on a computer, for the application proxy to instruct the NAT process to operate for the duration of an Internet application session utilizing
15 said real-time Internet protocol independent of data traffic flow.

09621250 " 092800